

# EXHIBIT 8

UNITED STATES DISTRICT COURT

for the  
Central District of California

In the Matter of the Search of )

(Briefly describe the property to be searched or identify the  
person by name and address)

Case No. 2:23-MJ-05295

A black LG Android cell phone, model number  
LGLS991, IMEI 357355062960973, in Federal  
Bureau of Investigations' ("FBI") custody; a silver  
Samsung cell phone with broken screen, model SM-  
J327p, in FBI's custody; and a gold LG cell phone  
with cracked screen, model LS990, serial  
#410KPVH0351583, in FBI's custody.

**WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California (identify the person or describe the property to be searched and give its location):

*See Attachment A*

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

*See Attachment B*

Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

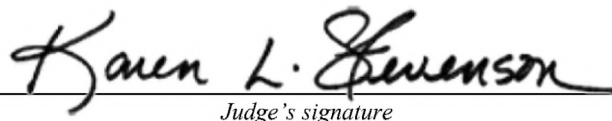
**YOU ARE COMMANDED** to execute this warrant on or before 14 days from the date of its issuance (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

You must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

Date and time issued: October 13, 2023, 1:49 p.m.

  
Judge's signature

City and state: Los Angeles, CA

Hon. Karen L. Stevenson, U.S. Magistrate Judge  
Printed name and title

AUSA: Alexandra Sloan Kelly, 213-894-5010

~~SECRET~~

## Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

## Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

### Executing *cjficer*'s signature

---

Printed name and title

**ATTACHMENT A**

PROPERTY TO BE SEARCHED

The following digital devices (the "SUBJECT DEVICES"), all of which were seized on March 9, 2018, and are currently in the custody of the FBI in Los Angeles, California:

- a. Black LG Android cell phone, model number LGLS991, IMEI 357355062960973;
- b. Silver Samsung cell phone with broken screen, model SM-J327P; and
- c. Gold LG cell phone with cracked screen, model LS990, serial #410KPVH0351583.

**ATTACHMENT B**

**I. ITEMS TO BE SEIZED**

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C § 2252A(a)(2) (receipt and distribution of child pornography) and 2252A(a)(5)(B) (possession of child pornography) (the "Subject Offenses"), namely:

a. Child pornography, as defined in 18 U.S.C. § 2256(8).

b. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer to child pornography, as defined in 18 U.S.C. § 2256(8), including but not limited to documents that refer to the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography.

c. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, tending to identify persons involved in the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, order, requesting, trade, or transaction of any kind, in interstate commerce, including by computer, involving any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(B).

d. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that identify any minor visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

e. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that discuss, depict, or evidence any minor engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

f. Any records, documents, programs, applications, messages, notes, materials, or items that are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings.

g. Any records, documents, programs, applications, notes, materials, or items, including electronic mail and electronic messages, which discuss or otherwise may be related to the sex exploitation of children.



h. Any records, documents, programs, applications, notes, materials, or items, including electronic mail and electronic messages, reflecting or evidencing communications with any minor.

i. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertain to Kik, including the use or creation of Kik accounts or users "Talleyhol14" or "Rusty Griswold."

j. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertain to accounts with any Internet Service Provider.

2. Any SUBJECT DEVICE which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

3. With respect to any SUBJECT DEVICE containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device;

g. records of or information about Internet Protocol addresses used by the device.

4. As used herein, the terms "records," "information," "documents," "programs," "applications," and "materials" include records, information, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

## **II. SEARCH PROCEDURE FOR THE SUBJECT DEVICES**

5. In searching the SUBJECT DEVICES (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any SUBJECT DEVICE capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.



b. The search team will, in its discretion, either search each SUBJECT DEVICE where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the SUBJECT DEVICES as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the digital devices and/or forensic images thereof beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each SUBJECT DEVICE capable of containing any of the items to be seized to the search protocols to determine whether the SUBJECT DEVICE and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK"

(Forensic Tool Kit), which tools may use hashing and other sophisticated techniques, including to search for known images of child pornography.

e. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

f. If the search determines that a SUBJECT DEVICE does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the SUBJECT DEVICE and delete or destroy all forensic copies thereof.

g. If the search determines that a SUBJECT DEVICE does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a SUBJECT DEVICE if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending),

including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the SUBJECT DEVICES, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

6. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.